BRITISH COLUMBIA SECURITIES COMMISSION
Securities Act, RSBC 1996, c. 418

Citation: Re Smillie, 2024 BCSECCOM 348 Date: 20240807

David Smillie and 1081627 B.C. Ltd. operating as ezBtc

Panel	Audrey T. Ho	Commissioner
	James Kershaw	Commissioner
	Marion Shaw	Commissioner
Hearing date	April 2, 3, 5 and 8, 2024	
Submissions completed	May 16, 2024	
Date of findings	August 7, 2024	
Appearing		
Jillian Dean Heesoo Kim	For the Executive Director	
Cody Reedman	For David Smillie	

Findings

I. Introduction

[1] This is the liability portion of a hearing under sections 161 and 162 of the *Securities Act*, 1996, c. 418 (Act).

[2] David Smillie (Smillie) and 1081627 B.C. Ltd. operating as ezBtc (ezBtc) are referred to collectively in these Findings as "the respondents".

[3] In a notice of hearing issued April 18, 2023 (2023 BCSECCOM 167), the executive director alleged, among other things, that:

a) the respondents perpetrated a fraudulent scheme relating to securities by lying to customers about a crypto asset trading platform the respondents claimed to operate and by diverting approximately $13 million in customer assets for their own purposes;

b) by engaging in the conduct set out in the notice of hearing, from December 2016 through September 2019 (the relevant period), the respondents contravened section 57(b) of the Act, as it then was; and

c) Smillie was the directing mind of ezBtc and therefore also contravened section 57(b) of the Act, pursuant to section 168.2(1) of the Act.

[4] ezBtc was dissolved in 2022 and did not participate in these proceedings. We find that notice has been effected in accordance with section 180 of the Act on ezBtc. Smillie was represented by legal counsel throughout these proceedings.

[5] On March 15, 2024, Smillie applied in writing to adjourn the liability hearing to an unspecified later date, to bifurcate the liability hearing into two stages and determine, in the first stage, whether the respondents' activities related to securities or derivatives, and to permit Smillie to attend the liability hearing and testify by videoconference.

[6] The executive director opposed the application to adjourn and to bifurcate the hearing.

[7] On March 26, 2024, we denied the application to adjourn and the application to bifurcate the hearing, with reasons to follow. We granted the application for Smillie to appear and testify by videoconference, contingent on a successful test of his remote environment.

[8] At the start of the liability hearing on April 2, 2024, Smillie through his legal counsel repeated his application to adjourn the hearing. The executive director opposed it. We dismissed the application orally, with reasons to follow.

[9] Our reasons relating to the dismissed applications are set out below.

[10] At the hearing, the executive director called as witnesses two commission staff members, four ezBtc customers and one expert witness.

[11] Smillie did not attend the hearing in person or by videoconference, but he was represented by legal counsel at the hearing. Smillie did not call any witness or tender any evidence. His counsel cross-examined the executive director's witnesses, and made written submissions after the hearing.

II. Factual Background

The respondents

[12] 1081627 B.C. Ltd. was incorporated in British Columbia on July 4, 2016. It was dissolved for failure to file on October 31, 2022.

[13] Smillie was a British Columbia resident during the relevant period. Searches of the corporate registry showed him as the incorporator and sole director of ezBtc on incorporation and as its sole director as at December 14, 2021 and September 20, 2022. There was no officer information provided as of any of those dates.

[14] Smillie was the sole authorized signatory of ezBtc's bank accounts at two financial institutions.

[15] Smillie represented himself variously as the founder, CEO, president or director of ezBtc when speaking with customers. One support staff member called him "the owner" when communicating with a customer. Smillie directly interacted with customers over email, text messaging, on chat platforms, on social media, by telephone and in person.

Cold and hot storage

[16] Conventional digital asset trading platform practice was to retain custody of a customer's crypto assets in digital wallets belonging to the platform. Assets were kept in "cold" wallets (or storage) for long-term storage, and "hot" wallets (storage) for short-term storage.

[17] A cold wallet is a place to store the private keys to an address on the blockchain, in a way that is disconnected from the Internet to make it safer from hacking. A blockchain address will have a balance of cryptocurrency. Each address is controlled by an individual or entity. To transfer

that balance to other blockchain addresses, one needs a private key (or password) to prove that one owns and controls that blockchain address.

The ezBtc platform

[18] ezBtc represented itself as operating a crypto asset exchange platform.

[19] ezBtc accepted the first customer deposits on the ezBtc platform in December 2016. It went offline permanently in or around September 2019. Between 2016 and 2019, customers deposited over 2,300 bitcoin and over 600 ether into their ezBtc addresses on the platform.

[20] On its website, ezBtc indicated that it:

a) offered a "unique savings program that allows customers to safely earn a 9% commission annually with daily payments"; and

b) stored over 99% of bitcoin and altcoins in cold storage.

[21] Smillie also told customers that crypto assets were kept in cold storage:

a) "I've taken extra precaution to segregate and cold store your coin";

b) "one of my biggest things has always been cold storage, cold storage, cold storage"; and

c) "to meet member demand, from time to time we have to retrieve crypto from that cold storage to supplement what's immediately on hand. It's extremely secure, but not a speedy process …".

[22] To use the ezBtc platform, a customer had to open an account online and then deposit fiat currency (cash) or cryptocurrency to a wallet address provided by ezBtc. ezBtc represented that it held the deposited cash or crypto assets on the customer's behalf.

[23] When a customer logged into their account, they could see, among other things, their account balance indicating the total amount of cash and crypto assets purportedly held by ezBtc on their behalf, their transaction history, and an order book listing buy and sell orders on the platform.

[24] A customer could buy crypto assets through the ezBtc platform using their deposited cash or crypto assets. Similarly, they could sell or trade crypto assets in their accounts through the platform for cash or other crypto assets. After each transaction, an entry would appear in the customer's account on the platform showing the resulting cash and crypto asset balance purportedly in their account.

[25] To withdraw crypto assets from the ezBtc platform, a customer was required to go online to request a withdrawal. ezBtc indicated that:

a) most coins were held in cold storage, and customers should expect 7-10 days for a standard withdrawal;

b) payments and withdrawals were processed manually; and

c) ezBtc may add a withholding period at its discretion on withdrawals based on member activity.

[26] ezBtc charged fees for deposits, withdrawals and trades.

ezBtc customers

[27] The commission received complaints from ezBtc customers when they could not withdraw their assets from ezBtc.

[28] Four customers testified and two other customers were interviewed under oath by a commission investigator (collectively "Testifying Customers"). They provided consistent evidence on:

a) their dealings with the ezBtc platform, such as: how to open an account; how to deposit, trade and withdraw assets; what they saw in their accounts;

b) their actual experience when they traded and tried to withdraw assets; and

c) their dealings with Smillie.

[29] Their evidence on how the ezBtc platform operated is reflected in the preceding section in these Findings.

[30] Testifying Customers deposited either or both crypto and fiat currencies on the ezBtc platform and traded on the platform. All except one of them confirmed they understood their crypto assets would be held by ezBtc in cold storage. Some complainants to the commission also mentioned that their crypto assets were to be held in cold storage.

[31] Testifying Customers had varying degrees of success in withdrawing crypto assets or cash purportedly held in their accounts. At some point, all encountered difficulties and none were able to withdraw all of the assets that ezBtc purportedly held for them.

[32] Smillie's name featured prominently in the Testifying Customers' dealings with ezBtc. Some complainants to the commission also mentioned Smillie.

[33] Customers who testified at the hearing described the negative emotional and financial impact on them. One had planned to use the funds to pay for certain medical procedures in his family and had to carry debt for a longer time to pay for them. He was the center of discussions or jokes among family and friends and had his intelligence questioned because he was defrauded.

[34] We highlight some of the key evidence from Testifying Customers in this section.

[35] Customer witness (JJ):

a) When JJ contacted the ezBtc website in 2017 to enquire about setting up an account to sell bitcoin, he received a reply from an ezBtc representative to send a note to "our owner, dave@ezbtc.ca", for advice.

b) JJ spoke to Smillie before depositing approximately 595 bitcoin on the ezBtc platform in April 2017. When JJ deposited them, Smillie told him that he would move JJ's bitcoin into cold storage for protection.

c) JJ understood that to process his withdrawal, ezBtc had to transfer the crypto assets from cold storage to hot storage, and then to a wallet elsewhere designated by him.

d) JJ immediately sold some of his bitcoin on the ezBtc platform for approximately $73,000. He asked ezBtc to transfer the money to his account. The money did not arrive.

e) JJ also requested a series of transfers from ezBtc to another cryptocurrency exchange. JJ had to enter a withdrawal request on the ezBtc platform and wait for Smillie to manually fulfill the withdrawal. The same ezBtc representative who had previously referred to Smillie as "owner" replied:

> With large withdrawals, we have our owner move the bitcoin over from cold storage so you can withdraw it. …

f) After text messaging with Smillie, 25 bitcoin were transferred to the other exchange.

g) When JJ tried to transfer his remaining bitcoin, Smillie told him that the ezBtc's website had been hacked and that approximately 484 of JJ's bitcoin had been stolen.

h) When JJ returned to Vancouver in May 2021, he met in person with Smillie and Smillie wrote him a $73,000 cheque in compensation for the bitcoin that JJ had previously sold on ezBtc.

i) JJ never recovered the 484 bitcoin. At the time, one bitcoin was selling for approximately $1,700 and JJ's financial loss then was approximately $823,000. At the time of this hearing, one bitcoin was worth approximately $100,000.

j) JJ testified that losing the bitcoin was very stressful. From the moment they went missing and for months afterwards, he thought about it every day. Later, when the price of bitcoin went up, he found it even more stressful. This experience affected his trust in crypto asset trading platforms as a whole.

[36] Customer RJ:

a) ezBtc had a program where it would give interest on deposits. RJ never took part in that.

b) RJ deposited bitcoin with ezBtc in April 2018 and sold them for Canadian dollars. He was paid the proceeds by cheque.

c) He made a second deposit of 0.2495 bitcoin on July 31, 2018, and sold them for $2,633.18. He requested a withdrawal on August 1 and followed up multiple times over the next eight months with ezBtc support and directly with Smillie. Despite repeated assurance from Smillie that he would be paid the next day or the next week, RJ never received the money.

d) Smillie threatened to sue RJ for libel for social media posts about his difficulty in getting withdrawals.

e) RJ sued the respondents in small claims court and was successful. He has not received payment on the judgement.

f) A tracing of RJ's 0.2495 bitcoin (see paragraph 41 below) shows that it was transferred from ezBtc to a gambling site 14 minutes after deposit by RJ.

[37] Customer MM:

a) MM deposited bitcoin and other cryptocurrencies with ezBtc multiple times in 2018. He also traded bitcoin for ether on the ezBtc platform where it was held.

b) He chose ezBtc because it promised a 9% return on cryptocurrencies held on the platform. MM wanted to earn interest on his holdings.

c) MM communicated with ezBtc support staff and Smillie directly multiple times when he tried to withdraw his assets in 2019. Despite their assurances, MM could not withdraw his bitcoin beyond miniscule amounts. He could not withdraw any of his ether.

[38] Around the time the ezBtc website went offline, Smillie stopped being responsive to customers. The commission investigator testified that Smillie was not interviewed as part of the investigation in this matter because enforcement staff could not locate him.

Forensic blockchain analysis

[39] The executive director retained Integra FEC LLC, a forensic data analytics and litigation consulting firm (Integra), to conduct a blockchain analysis to determine what happened to funds transferred from ezBtc's Bitcoin and Ethereum addresses. They were instructed to focus on two specific analyses:

a) calculation of the historical time balance of bitcoin and ether found in blockchain addresses belonging to ezBtc; and

b) the tracing of bitcoin and ether leaving the ezBtc platform.

[40] The analysis conducted by Integra and summarized in its report (the Expert Report) indicates that ezBtc did not retain custody of customers' assets in its Bitcoin and Ethereum digital addresses. Over 2,300 bitcoin and over 600 ether were deposited with ezBtc from 2016 to 2019. ezBtc quickly transferred incoming assets to the destinations listed in the below tables. The daily balance of ezBtc's Bitcoin and Ethereum wallets never exceeded 11 bitcoin and 20 ether respectively.

Bitcoin

	Destination	# of bitcoin transferred	Percentage of total
Bitcoin Group A	Smillie's accounts at crypto asset platforms Poloniex, Binance and Kraken (Smillie's Exchange Accounts)	123.53	5.24%
	CloudBet (online gambling site)	791.68	33.56%
	FortuneJack (online gambling site)	20.25	0.86%
	Subtotal Group A	935.46*	39.65%
*The notice of hearing refers to 935.47 bitcoin. Based on the entries in this table, 935.46 is the correct number and we have used that number in these Findings.			
Bitcoin Group B	Non-Smillie exchange accounts	773.85	32.80
	Other (transaction fees, miniscule transactions, amounts that did not reach an exchange within 10 hops)	650	27.55
	Subtotal Group B	1423.85	60.35%
	Total (Groups A+B)	2359.31	100%

Ether

Destination	# of ether transferred	Percentage of total
Smillie's Exchange Accounts	261	42.41%
Non-Smillie exchange accounts	187.44	30.46%
FortuneJack	159	25.84%
Other (amounts that did not reach an exchange within 5 hops)	8	1.30%
Total	615.44	100%

[41] To illustrate, the Expert Report described the tracing of a specific deposit of 0.2495 bitcoin made by customer witness RJ. The lead author and project manager for the Expert Report was David Lam. Lam testified that a unique feature of the Bitcoin blockchain allowed him to track the movement of that specific 0.2495 bitcoin. The tracing confirmed that RJ deposited 0.2495 bitcoin to the ezBtc platform. Fourteen minutes later, ezBtc transferred that exact same amount of bitcoin to CloudBet. RJ believed he sold his interest in that bitcoin for $2,633.18, but he was never able to withdraw those funds or recover the bitcoin.

[42] Integra also traced bitcoin as they left Smillie's Exchange Accounts. They found that large amounts of bitcoin were sent from Smillie's Exchange Accounts to CloudBet and FortuneJack. The Expert Report indicates:

a) Approximately 223 bitcoin were transferred from Smillie's Exchange Accounts to CloudBet and FortuneJack. This accounts for 58.1% of all bitcoin withdrawals from his analyzed exchange accounts;

b) Those 223 bitcoin exceeded the total (123.53) bitcoin transferred from ezBtc to Smillie's Exchange Accounts;

c) The flow of bitcoin from ezBtc to Smillie's Exchange Accounts corresponded with the flow of bitcoin from those accounts to CloudBet and FortuneJack. As more bitcoin came into Smillie's Exchange Accounts from ezBtc, more bitcoin were sent from Smillie's Exchange Accounts to the gambling sites. This is a strong indication that Smillie used funds from ezBtc to fund his accounts at those gambling sites;

d) The majority of ezBtc's transfers to CloudBet were to CloudBet accounts belonging to Smillie or an ezBtc insider. Over 21.3% of bitcoin transfers from ezBtc to CloudBet were made to CloudBet deposit addresses that also received bitcoin from Smillie's accounts at Poloniex, Binance and Kraken. A deposit address is a unique address on a digital platform that is provided to a given customer so that deposits from that customer can be identified as being by that customer. The fact that bitcoin transferred from both ezBtc and Smillie's Exchange Accounts were deposited into the same deposit address at CloudBet provides a strong indication that those ezBtc bitcoin transfers to CloudBet were made on behalf of Smillie. An additional 34.1% of bitcoin transfers to CloudBet were direct, single-output transfers which provides another strong indication that a significant portion of transactions were directed by Smillie or an ezBtc insider. When combining those two types of transfers from ezBtc to CloudBet, at least 55.4% of bitcoin transfers to CloudBet can be strongly inferred to have been made by Smillie or an ezBtc insider who had control of ezBtc's wallet addresses; and

e) Over 25% of bitcoin transfers from ezBtc to FortuneJack were made to FortuneJack addresses that also received bitcoin from Smillie's Exchange Accounts.

III. Preliminary Applications

March 15, 2024 application to adjourn and bifurcate hearing

[43] At a hearing management meeting on March 4, 2024, counsel for Smillie advised that Smillie believed the commission had issued a "no-action" letter in 2017 regarding the activities of ezBtc, or made representations that those activities were exempt from securities law. Counsel for the executive director indicated that she was unaware of the existence of such a letter but would order an expedited search for it and additional documents.

[44] On March 7, the executive director provided additional disclosure to Smillie (the March 7 disclosure). The March 7 disclosure included ten documents and totaled 41 pages. About ten of those pages were redacted as they related to other crypto asset trading platforms. Thirteen of those pages comprise a January 2018 letter from ezBtc's then counsel to the commission describing ezBtc's operations and setting out why the cryptocurrencies traded on its platform should not be treated as securities.

[45] On March 15, Smillie applied in writing to adjourn the liability hearing on the basis that he needed time to properly review the March 7 disclosure, that the March 7 disclosure had sparked an inquiry into additional documents that may be highly relevant to his defence, that he needed more time to seek additional documents that may not have been provided in the executive director's disclosure, and that he was not in Canada and had difficulty accessing records.

[46] Counsel for the executive director pointed out that there was no evidence from Smillie. The only evidence of the existence of a no-action letter was an affidavit from Mr. Reedman's legal assistant deposing that Mr. Reedman told the executive director's counsel in a March 1

telephone call that such a letter might exist. The executive director took the position that the documents disclosed on March 7 were irrelevant to the issues in these proceedings but were disclosed in a good-faith gesture to Smillie.

[47] The executive director provided affidavit evidence from the manager of the Legal Services department in the Capital Markets Regulation division of the commission. It was this individual and his team who communicated with ezBtc and Smillie in December 2017. The team sent communications to various crypto asset trading platforms in British Columbia seeking information about their operations in the course of a project to consider the jurisdiction that the commission should exercise over crypto asset trading platforms. The manager deposed that he did not send a no-action letter to the respondents, and it was not the practice of the Capital Markets Regulation division to send no-action letters or any letter with guarantees or assurances as to the commission's jurisdiction. After searching his own files and directing potentially involved team members to search their files, the manager could not locate any written correspondence with the respondents or their then counsel beyond the January 2018 letter from ezBtc's then counsel, and email communications in 2019 between Smillie and commission staff to set up a telephone call, commission staff notes on the call with Smillie, and commission staff notes on calls with other industry participants (redacted).

[48] *BC Policy 15-601 Commission Hearings* states, in subsection 3.4(c):

> ***(c) Adjournment Applications*** - The Commission expects parties to meet scheduled hearing dates. If a party applies for an adjournment, the Commission considers the circumstances, the timing of the application in relation to any hearing date, the fairness to all parties and the public interest in having matters heard and decided efficiently and promptly. The Commission will generally only grant adjournments if a panel is satisfied based on the evidence filed by the applicant that there are compelling circumstances. Where an adjournment application is based on a party's health, the Commission usually requires sufficient evidence from a medical professional.
>
> Where the Commission has previously set dates for a hearing, and a party retains new counsel, the Commission expects the new counsel to be available for those dates.

[49] We concluded that it was not in the public interest to adjourn the liability hearing. The limited evidence from Smillie was far from compelling. We were not persuaded that there would be prejudice or unfairness to Smillie in proceeding on the scheduled dates, and it was in the public interest to have matters heard and decided efficiently and promptly. Our primary reasons were:

a) Smillie provided no evidence to support the existence of the no-action letter, aside from a bare assertion made to his legal counsel. In contrast, we had extensive evidence from the executive director regarding staff's interactions with the respondents then and the searches conducted by the commission now to locate any such letter and related communications. We were not persuaded that a no-action letter existed or that there was correspondence from the commission giving assurance that ezBtc was not subject to securities law;

b) beyond asserting it, Smillie did not explain or provide any evidence on what it is about the March 7 disclosure that created a need for more time. The January 2018 letter that was disclosed was substantive, but it was clear that Smillie knew about it around the time it was sent. Moreover, that letter had little or no relevance, since it addressed a different issue and a different definition of "security" than what was alleged in the notice

of hearing. As a result, Smillie has not established that more time (than the three weeks between March 7 and April 2) was warranted to properly review the March 7 disclosure;

c) Smillie provided no evidence that he was abroad, or that he had difficulty accessing records, or why he could not return to Canada or direct someone who was present locally to access records for him during the nine months since the set-date hearing; and

d) the adjournment application was not timely. Smillie had been represented by the same counsel since at least the set-date hearing on June 27, 2023. The hearing dates were set with the concurrence of his counsel. The potential existence of a no-action letter was not raised until March 2024. Even if Smillie had difficulty retrieving records, given the significance of the purported no-action letter, we would expect him, as a director of ezBtc and the person who had the communications with commission staff, to recall far sooner the existence of such a letter and to take steps to search for it.

[50] With respect to the bifurcation application, Smillie argued that determining the core issue of whether the commission had jurisdiction would streamline the hearing and promote fairness and hearing efficiency. He said credibility would not be an issue since it would involve an assessment of the contracts and the nature of the crypto assets involved, and that it would benefit the commission to have focused submissions on this issue given that cryptocurrency exchanges and digital assets remained an evolving area. Smillie suggested that the first stage proceed on affidavit evidence and written submissions, together with limited examinations on the affidavits if necessary.

[51] The executive director opposed the application. He argued that bifurcation would not result in a clean segmentation of a preliminary issue from the body of the liability hearing. Determination of jurisdiction in this matter required a fact-driven analysis. A key concept in determining whether or not a particular agreement was a futures contract, as alleged by the executive director, was the timing of delivery of the underlying asset. This required a review of documentary evidence such as the terms of service as well as oral evidence on actual delivery practices. Bifurcation would duplicate the hearing process, as the executive director would require the same seven witnesses for both hearings.

[52] We concluded that it was not in the public interest to bifurcate the hearing. It is not uncommon for this commission to determine jurisdiction alongside liability in one hearing. Having a combined hearing would not reduce any focus on the jurisdictional issue. We agreed with the executive director that evidence from customer witnesses would likely be relevant to the jurisdictional issue as well as the fraud allegations, and bifurcation would create an overlap. We were also informed that all of the executive director's witnesses had set aside time to prepare for and attend the hearing. The commission had set aside days for the full hearing and it would be difficult to fill those days with other hearings on short notice. Bifurcating the hearing at this late stage was not efficient. Smillie had been on notice to defend the allegations in their entirety on the scheduled dates for over nine months, and did not ask for bifurcation until the last minute.

April 2, 2024 application to adjourn

[53] The April 2 application to adjourn was essentially on the same basis as the March 15 application, plus two more grounds:

a) Smillie's illness had made it difficult for his counsel to get instructions in the few weeks before the hearing; and

b) Smillie was impecunious and a three-month adjournment would provide him with time to raise money for his defence.

[54] Smillie did not tender any evidence.

[55] The executive director submitted that the application should be dismissed. There was no evidence to substantiate Smillie's illness, and no evidence to suggest that Smillie could find sufficient funds to proceed in three months.

[56] Counsel for Smillie indicated that he could not get instructions and did not have any information on Smillie's health issues. He advised that if the application were denied, he would not withdraw due to his professional obligations, but Smillie would not attend or testify at the hearing as he had originally planned to do. Counsel suggested that an adjournment might result in Smillie's participation.

[57] The panel denied the application. There was no evidence of Smillie's illness and how that affected his ability to participate in the hearing, especially when he was permitted to do so by videoconference. There was no evidence of his financial condition nor how that might improve in three or more months. An adjournment was not in the public interest.

Qualifying the expert witness

[58] The executive director sought to qualify Lam as an expert in forensic blockchain analysis. Smillie's counsel indicated he had not received instructions from Smillie and therefore took no position.

[59] Following direct and cross-examination of Lam on his education, work experience and knowledge, the panel qualified Lam as an expert in forensic blockchain analysis. The panel was satisfied that his testimony would be relevant to the allegations and necessary to the panel.

IV. Applicable Law

A. Standard of proof

[60] The standard of proof is proof on a balance of probabilities. In *F.H. v. McDougall*, 2008 SCC 53, the Supreme Court of Canada held, at paragraph 49:

> In the result, I would reaffirm that in civil cases there is only one standard of proof and that is proof on a balance of probabilities. In all civil cases, the trial judge must scrutinize the relevant evidence with care to determine whether it is more likely than not that an alleged event occurred.

[61] The Court also held at paragraph 46 that the "evidence must always be sufficiently clear, convincing and cogent to satisfy the balance of probabilities test".

[62] The Court went on to say, at paragraphs 47-48, that the evidence has to be weighed against the:

> … inherent improbability that an event occurred. Inherent improbability will always depend upon the circumstances.
>
> …There can be no rule as to when and to what extent inherent improbability must be taken into account … It will be for the trial judge to decide to what extent, if any, the

> circumstances suggest that an allegation is inherently improbable and where appropriate, that may be taken into account in the assessment of whether the evidence establishes that it is more likely than not that the event occurred.

[63] The panel is entitled to make inferences but may not speculate. As noted by the Alberta Court of Appeal in *Walton v. Alberta (Securities Commission)*, 2014 ABCA 273, at paragraph 27, quoting the underlying Alberta Securities Commission decision regarding circumstantial evidence:

> To summarize, when drawing an inference from circumstantial evidence, we must ensure that the inference is grounded on proved, not hypothetical or assumed, facts and is a reasonable one – one drawn using common sense, human experience and logic having considered the totality of the evidence and any competing inferences …

B. Relevant Legislation and Instruments

Relevant provisions of the Act and caselaw

[64] All references to the Act and multilateral instruments in these Findings are references to the versions that were in effect in British Columbia during the relevant period.

[65] Section 1(1) of the Act defined "security" to include:

> (n) an instrument that is a futures contract or an option but is not an exchange contract.

[66] "Futures contract" meant any obligation to make or take future delivery of

a) a commodity,

b) a security,

c) cash if the amount of cash is derived from, or by reference to, a variable including

i. a price or quote for a commodity or security,
ii. an interest rate,
iii. a currency exchange rate, or
iv. an index or benchmark,

but does not include an obligation, or a class of obligations, described in an order made under section 3.1.

[67] "Commodity" was defined as

a) any good, article, service, right or interest of which any unit is, from its nature or by mercantile custom, treated as the equivalent of any other unit;

b) the currency of any jurisdiction;

c) a gem, gemstone, or other precious stone; or

d) any other prescribed good, article, service, right or interest, or a class of any of those.

[68] "Exchange contract" was defined as a futures contract or an option that meets both of the following requirements:

a) its performance is guaranteed by a clearing agency; and

b) it is traded on an exchange pursuant to standardized terms and conditions set out in that exchange's bylaws, rules or regulatory instruments, at a price agreed on when the futures contract or option is entered into on the exchange, … .

[69] Section 57(b) of the Act stated:

> A person must not, directly or indirectly, engage in or participate in conduct relating to securities or exchange contracts if the person knows, or reasonably should know, that the conduct
>
> (b) perpetrates a fraud on any person.

[70] In *Anderson v. British Columbia Securities Commission*, 2004 BCCA 7, at paragraph 27, the British Columbia Court of Appeal summarized the elements of fraud:

> … the *actus reus* of the offence of fraud will be established by proof of:
>
> 1. the prohibited act, be it an act of deceit, a falsehood or some other means; and
> 2. deprivation caused by the prohibited act, which may consist in actual loss or the placing of the victim's pecuniary interests at risk.
>
> Correspondingly, the *mens rea* of fraud is established by proof of:
>
> 1. subjective knowledge of the prohibited act; and
> 2. subjective knowledge that the prohibited act could have as a consequence the deprivation of another (which deprivation may consist in knowledge that the victim's pecuniary interests are put at risk).

[71] In *Re Braun*, 2018 BCSECCOM 332, at paragraph 106, the commission held that the *mens rea* of a corporate defendant in fraud may be determined based upon the *mens rea* of the directors and officers of the corporation, particularly those who are directly responsible for managing or carrying out the affairs of the entity.

[72] Section 168.2 of the Act provided that if a corporate respondent contravened a provision of the Act, a person who was an employee, officer, director or agent of the corporation who "authorized, permitted or acquiesced" in the contravention also contravened the same provision of the Act.

[73] The commission in *Re Donald Bergman and others*, 2021 BCSECCOM 302, at paragraphs 38-39, considered the meaning of "authorized, permitted or acquiesced":

> There have been numerous decisions that have considered the meaning of the terms "authorize, permit, or acquiesce." In sum, these decisions require that the respondent have the requisite knowledge of the corporate contraventions and the ability to influence the actions of the corporate entity through action or inaction.

> In *Re Momentas Corp.*, 2006 ONSEC 15, the Ontario Securities Commission considered the meaning of "authorized, permitted, or acquiesced" for a director or officer's liability for the issuer's non-compliance with the Act, and stated at paragraph 118:
>
> > Although these terms have been interpreted to include some form of knowledge or intention, the threshold for liability under section 122 and 129.2 is a low one as merely acquiescing the conduct or activity in question will satisfy the requirement of liability. The degree of knowledge of intention found in each of the terms "authorize", "permit" and "acquiesce" varies significantly. "Acquiesce" means to agree or consent quietly without protest. "Permit" means to allow, consent, tolerate, given permission, particularly in writing. "Authorize" means to give official approval or permission, to give power or authority or to give justification.

[74] Section 8 of the *Interpretation Act*, RSBC 1996 c. 238 states:

> Every enactment must be construed as being remedial, and must be given such fair, large and liberal construction and interpretation as best ensures the attainment of its objects.

Multilateral Instrument 91-101

[75] Multilateral Instrument 91-101 *Derivatives: Product Determination* (MI 91-101) set out the types of over-the-counter derivatives that were subject to specific reporting requirements. It excluded from those reporting requirements certain categories of contracts and instruments (the excluded categories), including certain commodity contracts, that otherwise fell within the definition of "derivative" in MI 91-101.

CSA Staff Notice 21-327

[76] CSA Staff Notice 21-327 *Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets* (SN 21-327), published January 16, 2020, provides guidance from staff at the Canadian Securities Administrators (CSA) on the factors they consider to determine whether securities legislation applies to platforms that facilitate transactions relating to crypto assets, including the buying and selling of crypto assets (Platforms).

[77] SN 21-327 was issued after the relevant period. Staff notices do not have the force of law and are not binding on us. We refer to it because it aptly summarizes certain aspects of our independent assessment and conclusions about the nature of EzBtc's relationships with its customers and their respective rights and obligations with regard to the crypto assets purportedly held by ezBtc.

[78] CSA staff states, in SN 21-327, that "securities legislation may apply to Platforms that facilitate the buying and selling of assets, including crypto assets that are commodities, because the user's contractual right to the crypto asset may itself constitute a derivative."

[79] SN 21-327 cites the following situation as an example of where securities legislation does apply:

> We note that some Platforms purport to provide users with an opportunity to transact in crypto assets, including an opportunity to buy and sell crypto assets, but that, for several reasons, they retain ownership, control and possession of the crypto assets. They only require the users to transfer ownership, control and possession from the Platform's address to the user-controlled address upon the user's later request.

In these circumstances, there is no obligation to immediately deliver the crypto assets. Potentially, there will be ongoing reliance and dependence of the user on the Platform until the transfer to a user-controlled wallet is made. Until then, the user would not have ownership, possession and control of the crypto assets without reliance on the Platform. The user would be subject to ongoing exposure to insolvency risk (credit risk), fraud risk, performance risk and proficiency risk on the part of Platform.

For example, if the terms and conditions of a contract or instrument transacted on a Platform only require the Platform to transfer crypto assets to the user-controlled wallet on request (with the transaction simply recorded on the books of the Platform to evidence the purchase and the user's entitlement to receive the crypto asset on demand), the contract or instrument described above would be subject to securities legislation because:

- the contract or instrument does not create an obligation to make immediate delivery of the crypto assets to the user, and
- the typical commercial practice of the Platform is not to deliver, since users that do not make a request to transfer crypto assets do not receive full ownership, possession and control over the crypto assets that they transacted in.

In our view, a mere book entry does not constitute delivery, because of the ongoing reliance and dependence of the user on the Platform in order to eventually receive the crypto asset when requested.

V. Positions of the Parties on Liability

Executive director's position on jurisdiction

[80] In the notice of hearing, the executive director asserts that the respondents' alleged misconduct related to securities because the agreements between ezBtc and its customers (ezBtc agreements) were "futures contracts" and, as such, fell within the definition of "security" under section 1(1) of the Act. The executive director does not rely on any other definition of "security" in the Act to support his allegations.

[81] The executive director argues that bitcoin and ether are commodities, as one bitcoin is worth the same as any other bitcoin at any given moment in time, and the same is true for ether.

[82] The executive director submits that when a trade was executed on the ezBtc platform:

a) customers did not actually hold or trade their crypto assets – they held or traded a contractual right to a crypto asset;

b) the parties to the trade did not receive actual delivery of the crypto assets involved. Instead, an entry documenting the transaction was entered in their ezBtc accounts; and

c) there was no obligation or intention that customers must take delivery of crypto assets upon execution of a trade, or that ezBtc must make immediate delivery of the assets to the customers. Delivery occurred only at the election of the customer at some unspecified future date.

Therefore, when a customer deposited or acquired interests in a crypto asset on the ezBtc platform, ezBtc acquired an "obligation to make … future delivery" of the crypto asset at some

unspecified point to be determined by the customer. In other words, ezBtc entered into a "futures contract" with each of its customers.

[83] The executive director initially relied on MI 91-101 to support his arguments, but later changed his position. In reply submissions, the executive director argues that even if the ezBtc agreements fell within the excluded categories in MI 91-101, they were still "futures contracts" and "securities" under the Act. That is because MI 91-101 only exempted contracts in the excluded categories from reporting requirements for over-the-counter derivatives; it did not exclude them from the definition of "futures contract".

Smillie's position on jurisdiction

[84] Smillie argues that the relationships between ezBtc and its customers were not futures contracts and therefore, no security was involved. Since section 57(b) of the Act only governed conduct "relating to securities", there could be no violation of that section if no "security" was involved.

[85] Smillie's submissions focus almost entirely on MI 91-101. He submitted that the ezBtc agreements fit within the excluded categories under MI 91-101 for various reasons.

[86] Smillie also argues that bitcoin and ether do not constitute investment contracts as defined in *Pacific Coast Coin Exchange of Canada et al v. Ontario (Securities Commission) [1978] 2 SCR 112*, since customers had no expectation of profit arising from the efforts of others.

Executive director's position on fraud

[87] The executive director alleges in the notice of hearing that the respondents committed acts of deceit when they represented to customers that their crypto assets would be safely held in cold storage, but instead diverted a significant amount of customers' crypto assets for their own purposes.

[88] Specifically, the executive director alleges that ezBtc transferred 935.47 (935.46 in Bitcoin Group A table) of customers' bitcoin and 159 of customers' ether to two online gambling sites without customer authorization. The executive director did not make allegations about the transfer of 261 ether to Smillie's Exchange Accounts because no analysis was done on where they went after they left Smillie's Exchange Accounts.

[89] The total value of 935.47 bitcoin and 159 ether was $13 million as of July 1, 2019. The executive director used that date because the value of bitcoin and ether fluctuated significantly across the relevant period. July 1, 2019 was the approximate midpoint of customer complaints to the commission.

[90] The executive director submits that the respondents' actions not only put the customers' economic interests at risk, but caused actual losses to customers.

[91] The respondents had subjective knowledge of the deceit. They knew that they did not put customers' assets into cold storage. Smillie knew this because he controlled ezBtc and was the person who decided where to transfer customer assets. There is no evidence that someone else at ezBtc could have made the transfers without Smillie's knowledge. He knew that what he told customers about the storage of their assets was untrue.

[92] ezBtc knew this because its actions regarding storage of customer crypto assets were directed by Smillie, so Smillie's knowledge and state of mind should be attributed to it. The executive

director submits that where an individual controls a corporate respondent and perpetrates fraud, the individual's state of mind is attributed to the corporate respondent. He cited *Re Braun*, 2018 BCSECCOM 332 at paragraph 106, *Re Figueiredo*, 2016 BCSECCOM 233 at paragraphs 44, 48, 70.

[93] The respondents knew or ought to have known that their deceit in failing to keep customer assets in cold storage and instead transferring them to online gambling sites put those assets at risk and was likely to result in deprivation.

[94] With respect to section 168.2 of the Act, Smillie was the sole director, and the mind and management of ezBtc. He had the requisite level of knowledge and ability to influence the activities of ezBtc in order to have authorized, permitted or acquiesced to its contraventions.

Smillie's position on fraud

[95] Smillie concedes that ezBtc was improperly managed and operated negligently, but denies that he or ezBtc perpetrated a fraud.

[96] Smillie argues that the blockchain analysis was incomplete. There was no tracing done beyond CloudBet and FortuneJack. He suggests that it is plausible that the transferred bitcoin and ether were eventually returned to ezBtc. As well, no tracing was done to ascertain whether it was Smillie or someone else who executed the transfers. The executive director also did not address the extent to which the transfers represented actual customer transfers.

[97] Smillie denies that he was the controlling mind and management of ezBtc. For example, ezBtc had two other executives at one time, a chief financial officer and a senior support and compliance officer. He says the executive director had little knowledge of the inner workings of ezBtc and who controlled or had access to customer assets.

[98] With respect to liability under section 168.2 of the Act, Smillie submits there is no evidence that he authorized, permitted or acquiesced in the purported fraud.

[99] In the further alternative, Smillie argues that the executive director knew of ezBtc's existence as early as December 2017 and failed to take any enforcement action until 2019 when it issued an investigation order. The executive director's failure to take prompt enforcement action or alert ezBtc that it was subject to securities law resulted in substantial procedural unfairness to Smillie, and these proceedings should be dismissed.

VI. Analysis and Findings

Jurisdiction

[100] Since the executive director alleges that the respondents' conduct "related to securities" only by virtue of ezBtc entering into "futures contracts" with customers, we have jurisdiction only if we find that the ezBtc agreements were "futures contracts" under the Act.

[101] The parties did not provide any precedents, and the panel is not aware of any jurisprudence interpreting the definition of "futures contracts" on similar facts. In a recent decision, *LiquiTrade Ltd.*, 2024 BCSECCOM 292, this commission considered a crypto asset trading platform that appears to have similar features to ezBtc in key respects, but that decision addressed a different definition of "security" than "futures contract".

[102] We did not find the parties' submissions on MI 91-101 helpful. MI 91-101 has a limited and specific purpose that is not relevant here. Whether an instrument is excluded from reporting requirements for over-the-counter derivatives does not answer the question of whether it is a futures contract in the first place. MI 91-101 does not exclude a futures contract that falls within the excluded categories in MI 91-101 from the definition of "security" and the application of section 57(b) under the Act.

[103] Our analysis focuses instead on the explicit definitions contained in the Act. In doing so, we sought to give a fair and liberal interpretation to best attain the objectives of the Act.

[104] The parties do not dispute that the crypto assets at issue were "commodities". We agree that bitcoin and ether are commodities for the reasons stated by the executive director. One unit of bitcoin is, from its nature or by mercantile custom, treated as the equivalent of any other unit. The same is true for ether.

[105] There is also no dispute that the ezBtc agreements were not "exchange contracts". That is correct as the agreements were not guaranteed by a clearing agency.

[106] By the plain wording of the definition of a "futures contract", the key question we must answer is whether the ezBtc agreements contained an "obligation to make or take future delivery of" a commodity.

[107] Once a customer deposited their crypto assets on the ezBtc platform, they no longer had possession or control of the assets. The same was true for crypto assets that a customer acquired through the platform. The acquisition was simply recorded in their accounts at ezBtc to evidence the transaction and the customer's right to receive the crypto assets on demand. In each instance, the customer could not transfer, trade or deal with these assets except through ezBtc and through strict adherence with formal process requirements and the payment of fees. The customer could not obtain possession or control except by requesting a withdrawal on the platform and upon ezBtc transferring them to a customer-controlled wallet address. The customer's ability to deal with or obtain the assets was entirely dependent on ezBtc.

[108] We agree with the executive director on the proper characterization of the ezBtc agreements and the respective interests, rights and obligations of ezBtc and its customers. That characterization is also consistent with CSA staff's analysis as stated in SN 21-327. Without control over the assets and the ability to transfer, trade or deal with them as owner, all the customer had was an interest and a right, conferred by contract, to the number of crypto assets recorded in their account at ezBtc.

[109] The customer had a right to direct ezBtc to deliver to them the underlying crypto assets recorded in their account. But there was no obligation that customers must take delivery of the crypto assets upon the execution of a trade. Customers could maintain in their accounts their contractual interests in the underlying crypto assets and, at some indeterminate future point, elect to withdraw the underlying crypto assets. Similarly, there was no obligation on the part of ezBtc to make immediate delivery of the assets to which the customer has a claim on the execution of the contract or any other predetermined time. In fact, ezBtc offered a savings program for customers who kept their interests in crypto assets in their accounts and one customer (MM) testified that this feature enticed him to use the ezBtc platform.

[110] The obligation on ezBtc, and its stated commercial practice, was to deliver the underlying crypto assets when requested by the customer, which could be at some unspecified date in the future to be determined by the customer. Therefore, when a customer deposited or acquired contractual interests in a crypto asset on the ezBtc platform, they acquired a right to take future delivery of the underlying crypto asset, and ezBtc acquired an equal and offsetting "obligation to make future delivery" of the crypto asset to the customer.

[111] Although Smillie's submissions are directed at refuting the executive director's initial submissions on MI 91-101, we have considered the substance and reasoning underlying Smillie's submissions, to the extent applicable, in our analysis of the definition of "futures contract". In support of his position that the ezBtc agreements fell within the excluded categories under MI 91-101, Smillie argues that the parties intended and were obliged to settle their transactions by taking or making delivery of the underlying crypto assets, although delivery may not be immediate. He argues there is no requirement for immediate delivery, and a customer's decision on when to request withdrawal related solely to the *timing* of the delivery of the crypto asset and not to the obligation to do so. That argument flies against the plain wording of the definition of "futures contract" which expressly refers to an "obligation to make or take *future* delivery", so timing of delivery is very much a relevant consideration.

[112] Smillie also disagrees with the executive director's position that ezBtc customers only received contractual rights to the underlying crypto assets. He argues that true physical delivery, in the sense of a contracting party being given physical possession of an object, is not necessary to meet the requirements of MI 91-101, and that a commodity may be delivered by delivery of the instrument evidencing ownership of the commodity. In our view, delivery has not been made when customers lacked full ownership rights, possession and control of the crypto assets recorded in their accounts. Before withdrawal from the platform, they did not have access to wallet addresses to deal with the crypto assets independent of ezBtc. It was only when they requested a withdrawal that ezBtc was required to deliver the crypto assets to a customer-controlled wallet address that enabled them to deal with those assets. In our view, delivery was not made until that time.

[113] We did not find useful Smillie's submissions with respect to the *Pacific Coin* case, as that dealt with a different branch of the definition of "security" than was alleged by the executive director.

[114] For all the above reasons, we find that the ezBtc agreements were "futures contracts" and therefore "securities" as defined by section 1(1) of the Act.

Fraud

[115] We have reviewed the lengthy Expert Report detailing the blockchain analysis, the methodology used, the evidence and reasoning supporting the inferences made and conclusions reached. We had the benefit of hearing Lam's testimony directly. We find his testimony, the Expert Report and the inferences and conclusions in it logical, reasonable and persuasive.

[116] Following *Anderson*, we asked the following questions:

a) Was there a prohibited act?

b) If so, was deprivation caused by the prohibited act?

c) Did the respondents have subjective knowledge of the prohibited act?

d) Did the respondents have subjective knowledge that the prohibited act could have as a consequence the deprivation of its customers?

Was there a prohibited act?

[117] The evidence is clear, and we find that both ezBtc and Smillie represented to customers that their crypto assets will be safely held in cold storage. ezBtc did not do so. The evidence that ezBtc had no more than a daily balance of 11 bitcoin and 20 ether in its Bitcoin and Ethereum wallets proves that ezBtc did not keep custody of most of the bitcoin and ether that customers deposited, whether in hot or cold storage. It also supports the inference that the crypto assets transferred from ezBtc to gambling sites and Smillie's Exchange Accounts were customer crypto assets.

[118] We find that in aggregate, 935.46 bitcoin and 159 ether were transferred by ezBtc to Smillie's Exchange Accounts, and/or to CloudBet and FortuneJack. The transfers to the two gambling websites were sometimes direct from ezBtc, and sometimes indirect from ezBtc to Smillie's Exchange Accounts and then to the gambling websites.

[119] Customers deposited their assets with ezBtc so they could trade in crypto assets using the ezBtc platform. Their assets were not meant to be used for any other purpose. Diverting customers' assets to Smillie's Exchange Accounts or gambling sites while representing to customers that their assets were safely held by ezBtc in cold storage was deceitful and a prohibited act.

[120] Smillie asked us to infer that the crypto assets transferred to gambling websites were done on behalf of customers. That is not supported by evidence. It is not a reasonable inference that so many of its customers gambled on online sites, nor that so many of them would pay for their own gambling by routing their payments through ezBtc or Smillie's Exchange Accounts.

[121] Although the tracing stopped once assets were deposited with the gambling sites, there is no evidence to support Smillie's contention that those crypto assets could have been eventually returned to ezBtc. If that were true, why was ezBtc unable to repay customers? Even if that were true, the transfers to gambling sites and Smillie's Exchange Accounts were still contrary to their representations to customers to keep assets in cold storage and still put their customers' pecuniary interests at risk.

Was deprivation caused by the prohibited act?

[122] Customers were unable to recover all of their assets. The deceit led to actual loss.

Did Smillie have subjective knowledge of the prohibited act?

[123] Subjective knowledge is proven if Smillie knew that customers were told their crypto assets would be in ezBtc's custody and held in cold storage, but they were in fact transferred to gambling websites or to Smillie's personal accounts.

[124] ezBtc stated on its website that customer assets would be kept in cold storage. There is ample evidence that Smillie also made those representations to customers. He had subjective knowledge of what customers were told.

[125] Smillie intimates that others in ezBtc could have been responsible for diverting customer assets from ezBtc. He argues that he was not the controlling mind and management of ezBtc. That is not persuasive given his position, dominant role and level of involvement at ezBtc.

[126] Dealing first with those transfers to his personal accounts at Poloniex, Binance and Kraken, and those transfers from his personal accounts to CloudBet and FortuneJack, it is not credible that Smillie did not know about them. At the minimum, he would have been aware of and accepted those transfers.

[127] It is also not credible that he was unaware of those ezBtc transfers to the gambling site addresses that also received crypto assets from Smillie's Exchange Accounts. The fact that crypto assets from both ezBtc and Smillie's Exchange Accounts were deposited into the same deposit addresses at these sites leads us to conclude that it is more likely than not that he was aware of those transfers and they were made by him or on his behalf.

[128] The suggestion that others in ezBtc diverted customer assets without Smillie's knowledge or involvement is also not credible, when one considers that the persons who diverted the assets needed not only the private keys to ezBtc's wallets, but also the passwords and deposit addresses for Smillie's Exchange Accounts, and the deposit addresses for the two gambling sites that also received funds from Smillie's Exchange Accounts.

[129] The above is sufficient for us to find that Smillie had subjective knowledge that ezBtc did not keep custody of all of its customers' assets, and certainly not in cold storage, but instead diverted a significant portion to gambling sites and to his personal accounts.

[130] But we can go further. With respect to the remaining transfers to CloudBet and FortuneJack that were not deposited into the same addresses that received transfers from Smillie's Exchange Accounts, we conclude that it is more likely than not that Smillie was aware of them as well.

[131] Smillie is correct that the corporate searches on ezBtc only covered three dates and do not show that he was its sole director throughout the entire relevant period. As well, there were other people involved in operating ezBtc. But the evidence all points to Smillie as the key person at ezBtc. Support staff needed Smillie to move crypto assets from purported cold storage. There is no evidence that there was another person at ezBtc with similar authority and involvement as Smillie. Given his role at ezBtc, it is difficult to believe that someone else could have transferred a significant portion of ezBtc's assets without Smillie's knowledge.

[132] We are satisfied that Smillie had subjective knowledge that ezBtc did not keep custody of all of its customers' assets, and certainly not in cold storage, but instead diverted all of the transfers in question to gambling sites or to his personal accounts.

[133] Although our reasoning would have supported a finding that the prohibited act included the transfer of 261 ether to Smillie's Exchange Accounts, we have not done so as that was not alleged by the executive director.

Did Smillie have subjective knowledge that the prohibited act could lead to deprivation?

[134] It is obvious that Smillie ought to have known that transferring customers' assets to his personal accounts and to online gambling sites, instead of keeping them at ezBtc in cold storage, could result in the loss of those assets and put the customers' pecuniary interest at risk.

Did ezBtc have subjective knowledge of the prohibited act and that it could lead to deprivation?

[135] Smillie was the founder and self-styled president of ezBtc. He was the sole director for at least some if not the entire time during the relevant period. Customers dealt with him primarily outside of technical support. The evidence supports the conclusion that Smillie was directly responsible for managing and carrying out the affairs of ezBtc. There is no evidence that there was another person at ezBtc with similar authority and involvement as him. It is more likely than not that Smillie was the one who directed the affairs of ezBtc, and we could attribute his subjective knowledge to ezBtc.

[136] We therefore find that both respondents have contravened section 57(b) of the Act.

[137] On the issue of procedural fairness raised by Smillie, we agree with the executive director that the respondents could not have a legitimate expectation that they could deceive customers and deprive them of their assets because the respondents were not told that their platform was subject to securities law.

[138] Smillie also submitted that the commission failed to take prompt enforcement action and that resulted in procedural unfairness. The December 2017 date referred to in Smillie's submissions on procedural fairness was the date when the regulatory division of the commission wrote to ezBtc seeking information about its operations, as part of an initiative to better understand the crypto industry. Most of the customer complaints to the commission were received in 2019. The approximate midpoint of customer complaints to the commission was July 2019. An investigation order was obtained in August 2019. In light of that timing, we do not find any undue delay.

Section 168.2 liability

[139] Given our finding that Smillie contravened section 57(b), it is not necessary to make a finding under section168.2 as well. But for the reasons already stated, we are persuaded that Smillie was at minimum aware of, and likely directed, the transfers of customer assets. As director and self-styled president, and the one who directed the affairs of ezBtc, he was in a position to influence that action. At minimum, he "permitted or acquiesced" in the contravention by ezBtc and so, he also contravened section 57(b) by virtue of section 168.2 of the Act.

VII. Summary of Conclusions

[140] In conclusion, we find that:

a) the respondents perpetrated a fraud relating to securities by lying to customers about holding their crypto assets in cold storage in ezBtc's custody, but instead diverting 935.46 customer bitcoin and 159 customer ether for their own purposes;

b) by doing so, the respondents contravened section 57(b) of the Act; and

c) Smillie also contravened section 57(b) of the Act, pursuant to section 168.2(1) of the Act.

VIII. Submissions on Sanction

[141] We direct the executive director and the respondents to make their submissions on sanctions as follows:

By September 3, 2024	The executive director delivers submissions to Smillie and the Commission Hearing Office.
By September 17, 2024	Smillie delivers response submissions to the executive director and the Commission Hearing Office. Any party seeking an oral hearing on the issue of sanctions so advises the Commission Hearing Office. The hearing officer will contact the parties to schedule the hearing as soon as practicable after the executive director delivers reply submissions (if any).
By September 24, 2024	The executive director delivers reply submissions (if any) to Smillie and to the Commission Hearing Office.

August 7, 2024

For the Commission

Audrey T. Ho
Commissioner

James Kershaw
Commissioner

Marion Shaw
Commissioner